CLAIMS

I claim:

a1

1. A method comprising the steps of:

encrypting a data message m using a primary transmitter secret key z to form a quantity E;

preparing a quadruplet (a_{new}, b_{new}, s_{new}, E) where:

$a_{new} = z^* y^c$ modulo p ;
$b_{new} = g^c$ modulo p;
s_{new} = signature $_c(a_{new}, b_{new}, E)$;

where $y = g^x$ modulo p, c is a random number, x is a receiver secret key, and the parameters g, x, and p are picked using a known encryption method;

verifying the signature s_{new};

decrypting a_{new} and b_{new} using the receiver secret key x to get the primary transmitter secret key z;

using the primary transmitter secret key z to decrypt the quantity E and thereby obtaining the message m.

2. The method of claim 1 and wherein:

the step of decrypting a_{new} and b_{new} using the receiver secret key x to get the primary transmitter secret key z is comprised of computing $z = a_{new}/b_{new}^{\ x}$.

3. The method of claim 1 wherein:

El Gamal encryption is used for the encrypting steps.

a

4. The method of claim 2 wherein:

El Gamal encryption is used for the encrypting steps.

5. The method of claim 1 wherein:

the primary transmitter secret key z is determined from the formula of $z = g^{\gamma}$ modulo p, where γ is a random value chosen from the set [0..q], where q is a value picked using a known encryption method.

6. A method comprising the steps of:

creating a primary transmitter key z;

creating a secondary transmitter key z' which is a function of z;

encrypting a data message m using the secondary transmitter secret key z' to form a quantity E;

preparing a quadruplet (a_{new}, b_{new},s_{new}, E) where:

$a_{new} = z^* y^c$ modulo p ;
$b_{new} = g^c$modulo p;
s_{new} = signature $_c(a_{new},b_{new},E)$;

where $y = g^x$ modulo p, c is a random number, x is a receiver secret key, and the parameters g, x, and p are picked using a known encryption method;

verifying the signature s_{new};

decrypting a_{new} and b_{new} using the receiver secret key x to get the primary transmitter secret key z;

a'

modifying the primary transmitter secret key z to obtain the secondary transmitter secret key z' and using the secondary transmitter secret key z' to decrypt the quantity E and thereby obtaining the message m.

7. The method of claim 6 and wherein:

the primary transmitter key z is provided which is not of the format used for producing the ciphertext E;

the secondary transmitter key z' is computed as a function of z, where the function is an arbitrary function.

8. A method comprising the steps of:

creating a primary transmitter key z;

creating a secondary transmitter key z' which is a function of z;

providing a plurality of portion keys which are derived from the secondary transmitter key z';

encrypting a data message m using the plurality of portion keys to form a quantity E;

preparing a quadruplet (a_{new}, b_{new}, s_{new}, E) where:

$a_{new} = z^* y^c$ modulo p ;
$b_{new} = g^c$modulo p;
s_{new} = signature $_c(a_{new}, b_{new}, E)$;

where $y = g^x$ modulo p, c is a random number, x is a receiver secret key, and the parameters g, x, and p are picked using a known encryption method;

a'

verifying the signature s_{new};

decrypting a_{new} and b_{new} using the receiver secret key x to get the primary transmitter secret key z;

modifying the primary transmitter secret key z to obtain the secondary transmitter secret key z' and using the secondary transmitter secret key z' to determine the plurality of portion keys and using the plurality of portion keys to decrypt the quantity E and thereby obtaining the message m.